Pentesting Lab

Active Directory Intro

Ostermayer, Possegger, Pongratz, Schauklies, Schwarzl

19.03.2026

Summer 2026, www.isec.tugraz.at/ptl

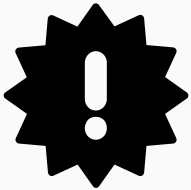
Table of contents

1. Introduction

2. The Core Structure

3. The Attack Landscape

Introduction



- Since this is a pentesting course, we will focus on attack points on Active Directory
- Therefore, many concepts and technical details will be wildly simplified and/or omitted!
- However, you should know what you attacked and why it worked, especially in the submission reviews.
- If you want to learn more, check out this Microsoft Learn Path:
- https://learn.microsoft.com/en-us/training/paths/active-directory-domain-services/

What is Active Directory?

- Active Directory is a directory service for (Windows) domain networks.
- It is a collection of ”Roles” that can be assigned to one or many Windows Servers:
  - Active Directory Domain Services
  - Active Directory Federation Services
  - Active Directory Certificate Services
  - There are more!
- It is based on standard technologies
  - LDAP (Lightweight Directory Access Protocol)
  - Kerberos
  - DNS (Domain Name System)
  - SMB (Server Message Block)

A Brief History

- Released with Windows 2000 Server edition
- Support retrofitted back to Windows 95
- Features and security have been greatly enhanced since then
- Still needs to be backwards compatible
- That's were the problems start:
  - Old Operating Systems do not support modern encryption
  - They only support insecure protocols
  - They cannot work with modern Hashing-Algorithms
  - etc.

Why (pentest) Active Directory?

- About 90% of Fortune 1000 companies use Active Directory[1]
- You are almost guaranteed to encounter it in an internal pentest
- Active Directory can do everything an administrator needs
- But does everyone know how to configure everything properly?
- Very hard to do everything right
  - A single mistake can lead to disaster
  - There are checkboxes that (if checked) lead to instant domain compromise for every user!

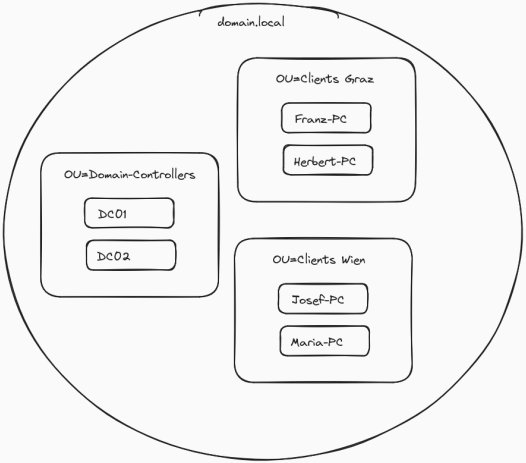
[1] https://www.frost.com/frost-perspectives/active-directory-holds-the-keys-to-your-kingdom-but-is-it-secure/

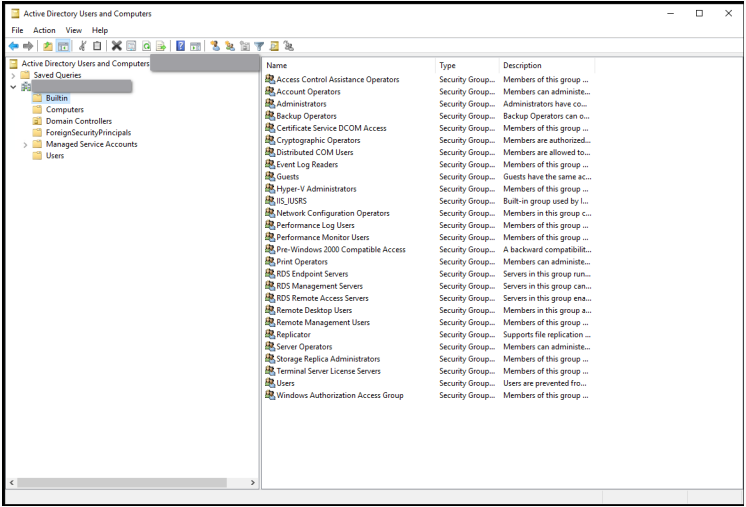
The Core Structure

Roles

- Active Directory Domain Services
  - Hosted on a Domain Controller
  - Users & Groups
  - Organizational Units
  - Group Policies
  - Access Control
  - etc.
- Active Directory Certificate Services
  - Should be a different server (sometimes it's hosted on a DC, bad!)
  - Certificate Management
  - Issuing certs based on templates
  - Certificates are used for Encryption, Signing and Authentication

- Domain(s)
  - A logical grouping of network objects (users, computers, groups)
  - Establishes boundaries and ACLs
  - Organizational Units (OUs)
    - Hierarchically managed containers
    - Grouping similar assets together (e.g. Client-Workstations)
- Forest(s)
  - Group of Domains
  - Sharing a common schema and configuration

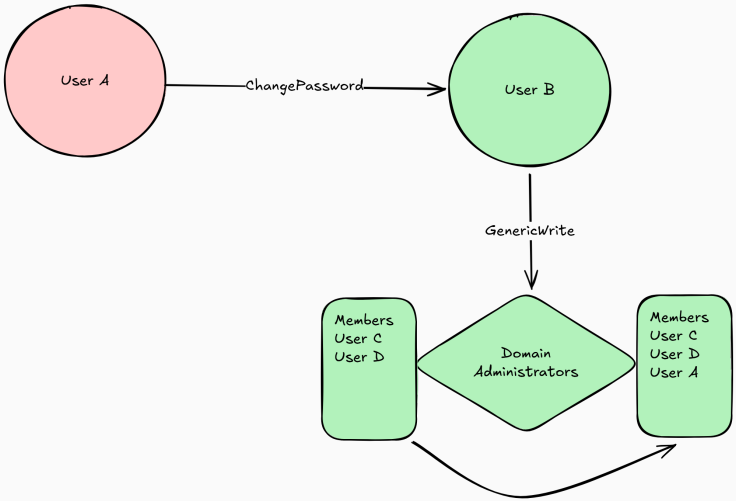

domain.local
OU=Clients Graz
Franz-PC
Herbert-PC
OU=Domain-Controllers
DC01
DC02
OU=Clients Wien
Josef-PC
Maria-PC


Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers
Saved Queries
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Name
Type
Description
Access Control Assistance Operators
Security Group...
Members of this group ...
Account Operators
Security Group...
Members can administe...
Administrators
Security Group...
Administrators have co...
Backup Operators
Security Group...
Backup Operators can o...
Certificate Service DCOM Access
Security Group...
Members of this group ...
Cryptographic Operators
Security Group...
Members are authorized...
Distributed COM Users
Security Group...
Members are allowed to...
Event Log Readers
Security Group...
Members of this group ...
Guests
Security Group...
Guests have the same ac...
Hyper-V Administrators
Security Group...
Members of this group ...
IIS_IUSRS
Security Group...
Built-in group used by I...
Network Configuration Operators
Security Group...
Members in this group c...
Performance Log Users
Security Group...
Members of this group ...
Performance Monitor Users
Security Group...
Members of this group ...
Pre-Windows 2000 Compatible Access
Security Group...
A backward compatibilit...
Print Operators
Security Group...
Members can administe...
RDS Endpoint Servers
Security Group...
Servers in this group run...
RDS Management Servers
Security Group...
Servers in this group can...
RDS Remote Access Servers
Security Group...
Servers in this group ena...
Remote Desktop Users
Security Group...
Members in this group a...
Remote Management Users
Security Group...
Members of this group ...
Replicator
Security Group...
Supports file replication ...
Server Operators
Security Group...
Members can administe...
Storage Replica Administrators
Security Group...
Members of this group ...
Terminal Server License Servers
Security Group...
Members of this group ...
Users
Security Group...
Users are prevented fro...
Windows Authorization Access Group
Security Group...
Members of this group ...

- Users represent individual accounts (also service accounts)
- Groups can contain users, computers **and other groups**
- Important built-in privileged groups:
  - **Domain Admins**: full control over the domain
  - **Enterprise Admins**: full control over all forest domains
  - **Schema Admins**: can modify the AD schema (can break stuff completely)
  - **Administrators**: local admin on domain controllers
  - **Account Operators, Backup Operators, * Operators etc.**
- Special account: **krbtgt**
  - Kerberos service account
  - Its NTLM hash is used to sign every Kerberos ticket in the domain
  - Compromising it = compromising the entire domain (Golden Ticket)

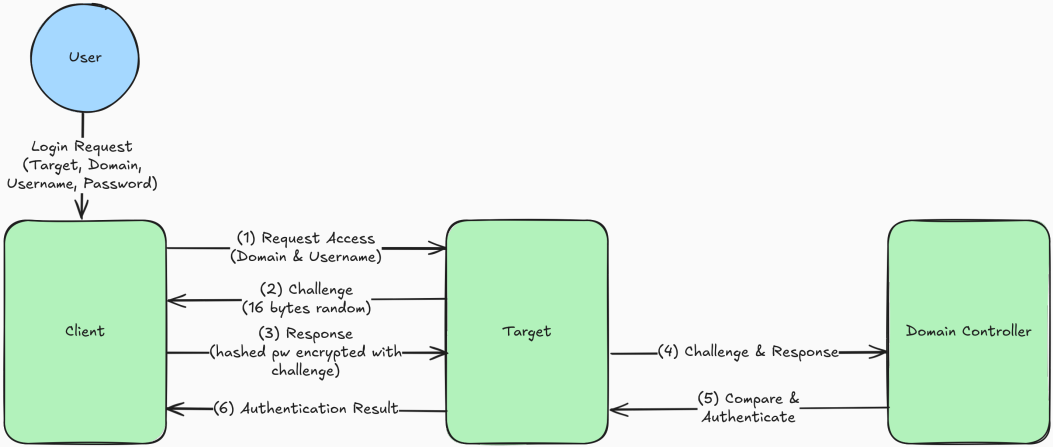
- Group Policies can enforce settings and configurations on users and computers
- Set registry settings, run startup and login scripts, deploy and manage software, etc.
- Can be applied at the Domain, OU, and Group level
- Examples:
  - Enforce a screen lock after 5 minutes of inactivity
  - Harden some security settings, like disallowing RC4 encryption
  - Map network drives with a login script (good idea?)
  - Run a software install script with a pre-configured admin account (good idea?)

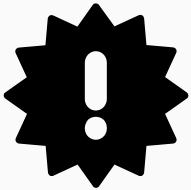
- Every AD object (user, group, computer, GPOs, etc.) can be protected by ACLs
- A list of entries that allow or deny permissions to that object
- Some sensitive permissions:
  - **GenericAll**: full control (read, write, delete, take ownership)
  - **WriteDACL**: modify the ACLs (grant yourself permissions)
  - **WriteOwner**: change ownership (to yourself for example)
  - **ForceChangePassword**: reset the account's password (Helpdesk users)
  - **GenericWrite**: write arbitrary attributes (e.g. add a user to a group)
- These are frequently misconfigured – a helpdesk user having `GenericAll` over a Domain Admin is not rare!


User A
ChangePassword
User B
GenericWrite
Members
User C
User D
Domain
Administrators
Members
User C
User D
User A

- LDAP
  - Common interface for all Active Directory queries
  - Only on Domain Controllers
  - Ports: 389/tcp (LDAP) or 636/tcp (LDAPS)
- DNS
  - Resolving Domain Names to IP Addresses
  - Crucial for a working environment (Kerberos, Certificates etc.)
  - Usually also on Domain Controllers
  - Ports: 53/udp
- SMB
  - Used for fileshares and remote administration
  - Tightly connected and required for Group Policies and Startup Scripts
  - Open on most machines
  - Ports: 137-139/tcp & 445/tcp

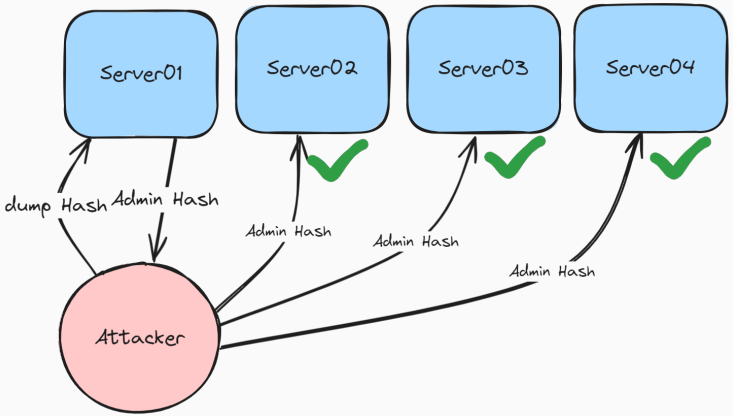
- Either via NTLM (legacy)
- Or Kerberos (modern)
- NTLM is considered insecure and allows lots of attacks
- However, it is still widely in use today and it is not recommended to turn it off
- Kerberos is more modern but has some problems too

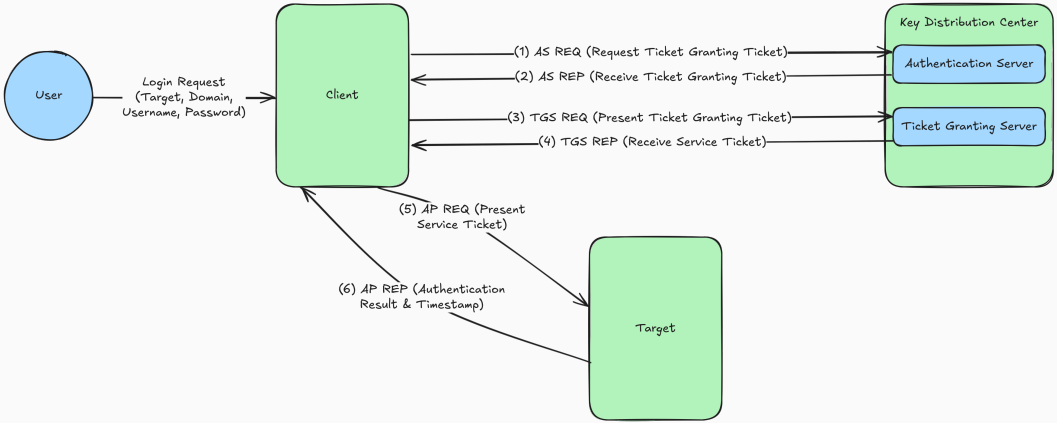

User
Login Request
(Target, Domain,
Username, Password)
Client
(1) Request Access
(Domain & Username)
(2) Challenge
(16 bytes random)
(3) Response
(hashed pw encrypted with
challenge)
(6) Authentication Result
Target
(4) Challenge & Response
(5) Compare &
Authenticate
Domain Controller



NTLM != NTLM

- NTLM-Hashes are used in Windows and therefore Active Directory
- They are based on MD4 and are not salted (yes, really)
- Local accounts and also domain accounts have NTLM-Hashes (stored on the Domain Controller)
- NTLM-Authentication does not use the NTLM-Hash directly, but a derived value called NTLMv2-Hash
- An NTLM-Hash can be used to authenticate without knowing the password (Pass-The-Hash attack)


Server01
Server02
Server03
Server04
dump Hash
Admin Hash
Admin Hash
Admin Hash
Admin Hash
Attacker


User
Login Request
(Target, Domain,
Username, Password)
Client
(1) AS REQ (Request Ticket Granting Ticket)
(2) AS REP (Receive Ticket Granting Ticket)
(3) TGS REQ (Present Ticket Granting Ticket)
(4) TGS REP (Receive Service Ticket)
Key Distribution Center
Authentication Server
Ticket Granting Server
(5) AP REQ (Present
Service Ticket)
(6) AP REP (Authentication
Result & Timestamp)
Target

NTLM

- Challenge-response
- Client proves knowledge of password hash by encrypting challenge
- Server forwards challenge to DC for verification

Kerberos

- Ticket-based protocol (TGT → Service Ticket)
- KDC (on DC) issues tickets, server validates without DC
- Service tickets encrypted with hash of service account (mostly AES256)

The Attack Landscape

- Pwning an AD environment follows a pattern:
  1. **Foothold**: obtain valid credentials or an initial access point
     - You usually get this from the customer, like a low-priv user or workstation
  2. **Enumeration**: domains, users, computers, groups, fileshares, ACLs, GPOs, etc.
  3. **Privilege Escalation**: gain more access from the low-priv account
  4. **Lateral Movement**: go from machine to machine until you reach more sensitive systems
  5. **Domain Compromise**: obtain Domain Admin or access the Domain Controller
- Privilege Escalation and Lateral Movement go hand in hand and are a longer process

Active Directory exercise: With what you already know, try to identify potential security problems, misconfigurations, attack paths etc. Map them to each phase: Enumeration, Privilege Escalation, Lateral Movement and Domain Compromise. Bonus for Foothold

Doesn't have to be too technical! We will then compare it to what I have seen.

What I Have Seen

- All Domain Users having local admin on ALL workstations (not just their own).
- One password for all service accounts that never expires (three characters).
- A backup account with its password in its description attribute (one character)
- Printer scans documents to a share. Using a Domain Admin account.
- Logon scripts in a Group Policy that mounts a file share with cleartext domain account.
- All computers are in a group that is in another group, that is in another group [...] that is in Domain Admins.
- Users can request a certificate (think of ACME), but they can specify any name for it. (Certificates can be used for authentication)

- Most attacks exploit misconfigurations, not technical vulnerabilities
- Those misconfigurations are often the default setting though
- You are not pentesting against code, but mostly human mistakes and bad practices
- AD admins have to manage thousands of objects, all of them have ACLs
- Authentication is tightly coupled: one compromised account can allow pivoting
- Active Directory was designed before many of today's threat models existed
- A single checkbox in the wrong place can mean instant Domain Admin for any user